



PATENT

Docket No. JCLA10645

page 1

IN THE UNITED STATE PATENT AND TRADEMARK OFFICE

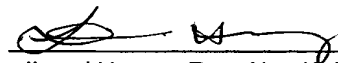
In re application of : MIN-CHIH HSUAN et al.
Application No. : 10/666,802
Filed : September 17, 2003
For : SYSTEM, METHOD AND CHIP FOR
HARDWARE DETECTION OF ILLEGAL
SOFTWARE USER, COMPUTER
SYSTEM HAVING HARDWARE
DETECTION CHIP THEREOF AND A
SOFTWARE REGISTRATION CENTER

Certificate of Mailing

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as certified first class mail in an envelope addressed to: Commissioner for Patents, P.O.BOX 1450, Alexandria VA 22313-1450, on

February 3, 2004

(Date)


Jiawei Huang, Reg. No. 43,330

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Transmitted herewith is a certified copy of **Taiwan** Application No. **92124297** filed on **September 03, 2003**.

A return prepaid postcard is also included herewith.

It is believed no fee is due. However, the Commissioner is authorized to charge any fees required, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 50-0710 (Order No. JCLA10645).

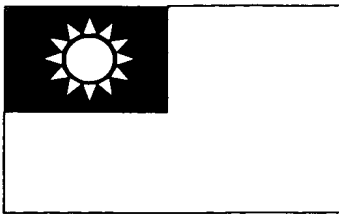
Date: 2/3/2004

By: 
Jiawei Huang
Registration No. 43,330

Please send future correspondence to:
J. C. Patents
4 Venture, Suite 250
Irvine, California 92618
Tel: (949) 660-0761

10/666.802

SCIA 10645



中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下：

This is to certify that annexed is a true copy from the records of this
office of the application as originally filed which is identified hereunder:

申請日：西元 2003 年 09 月 03 日
Application Date

申請案號：092124297
Application No.

申請人：聯華電子股份有限公司
Applicant(s)

局 長

Director General

蔡練生

發文日期：西元 2003 年 11 月 12 日
Issue Date

發文字號：09221141650
Serial No.

申請日期：	IPC分類
申請案號：	

(以上各欄由本局填註)

發明專利說明書

一、 發明名稱	中 文	應用硬體偵測非法軟體載入之系統、方法、及其使用之晶片、與具有該晶片之電腦系統及一軟體註冊中心
	英 文	SYSTEM, METHOD AND CHIP FOR HARDWARE DETECTION OF ILLEGAL SOFTWARE USER, COMPUTER SYSTEM HAVING HARDWARE DETECTION CHIP THEREOF AND A SOFTWARE REGISTRATION CENTER
二、 發明人 (共1人)	姓 名 (中文)	1. 宣明智
	姓 名 (英文)	1. Min-Chih Hsuan
	國 籍 (中英文)	1. 中華民國 TW
	住居所 (中 文)	1. 新竹科學園區竹村二路12之4號
	住居所 (英 文)	1. No. 12-4, Chu-Tsun II Rd., Science-Based Industrial Park, Hsinchu, Taiwan, R.O.C.
三、 申請人 (共1人)	名稱或 姓 名 (中文)	1. 聯華電子股份有限公司
	名稱或 姓 名 (英文)	1. United Microelectronics Corp.
	國 籍 (中英文)	1. 中華民國 TW
	住居所 (營業所) (中 文)	1. 新竹科學工業園區新竹市力行二路三號 (本地址與前向貴局申請者相同)
	住居所 (營業所) (英 文)	1. No. 3, Li-Hsin Rd. II, Science-Based Industrial Park, Hsinchu, Taiwan, R.O.C.
	代表人 (中文)	1. 曹興誠
	代表人 (英文)	1. Robert H.C. Tsao



四、中文發明摘要 (發明名稱：應用硬體偵測非法軟體載入之系統、方法、及其使用之晶片、與具有該晶片之電腦系統及一軟體註冊中心)

一種軟體版權保護之系統、方法、晶片與周邊系統，係使用一智慧型安全身份(Smart security-ID, "SID")積體電路(Integrated Circuit)。使用者為了取得合法之使用權，需將軟體之序號與使用者電腦之一通訊設備序號，註冊至該智慧型安全身份積體電路中，以取得一合法之檢查碼。該智慧型安全身份積體電路可做為一序號內建模組(built-in module)。同時該序號內建模組亦可在有非法使用者以非法之方式註冊時，通知該軟體之製造廠商。

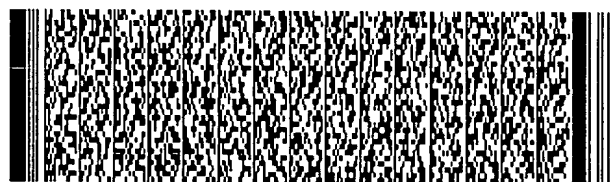
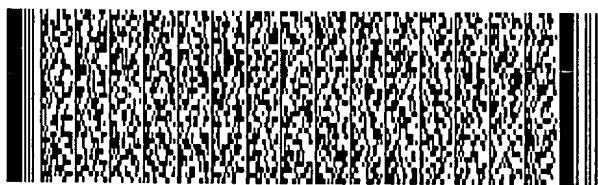
伍、(一)、本案代表圖為：第____3____圖

(二)、本案代表圖之元件代表符號簡單說明：

10：電腦	100：通訊設備	102：身份辨識電路
104：通訊控制介面	106：微處理器	108：記憶體
110：媒體存取控制器	112：非揮發性記憶體	
114：新產品註冊中心	116：資料庫	118：軟

六、英文發明摘要 (發明名稱：SYSTEM, METHOD AND CHIP FOR HARDWARE DETECTION OF ILLEGAL SOFTWARE USER, COMPUTER SYSTEM HAVING HARDWARE DETECTION CHIP THEREOF AND A SOFTWARE REGISTRATION CENTER)

A software copyright protection system, method, chip and peripheral subsystem are provided. In one aspect of the system and method, a smart security-ID ("SID") integrated circuit ("IC") is used for registering a legal user ID. The SID IC can work as a hardware serial number (S/N) built-in module and is combined with a soft S/N to protect the intelligent property ("IP") of



四、中文發明摘要 (發明名稱：應用硬體偵測非法軟體載入之系統、方法、及其使用之晶片、與具有該晶片之電腦系統及一軟體註冊中心)

體製造商

六、英文發明摘要 (發明名稱：SYSTEM, METHOD AND CHIP FOR HARDWARE DETECTION OF ILLEGAL SOFTWARE USER, COMPUTER SYSTEM HAVING HARDWARE DETECTION CHIP THEREOF AND A SOFTWARE REGISTRATION CENTER)

the software. The hardware S/N built-in module can also inform the software producer when any illegal user is trying to register the software.



一、本案已向

國家(地區)申請專利

申請日期

案號

主張專利法第二十四條第一項優先權

無

二、☐主張專利法第二十五條之一第一項優先權：

申請案號：

無

日期：

三、主張本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間

日期：

四、☐有關微生物已寄存於國外：

寄存國家：

寄存機構：

寄存日期：

寄存號碼：

無

☐有關微生物已寄存於國內(本局所指定之寄存機構)：

寄存機構：

寄存日期：

寄存號碼：

無

☐熟習該項技術者易於獲得, 不須寄存。



五、發明說明 (1)

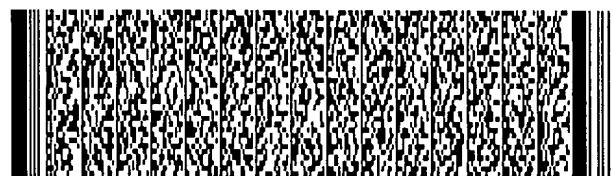
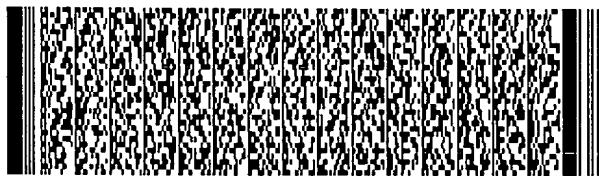
發明所屬之技術領域

本發明是有關於一種偵測非法軟體載入之方法，且特別是有關於一種應用硬體偵測非法軟體載入的積體電路元件的設計方法。

先前技術

在習知的軟體版權保護方法中，一般是使用以軟體序號(serial number, "S/N")來註冊之方法。在習知中最簡單的註冊方法，是軟體製造廠商，在該軟體出版時，在其中有一檔案或複數個檔案中，儲存有複數個軟體序號，或複數個註冊碼(register code)。對一使用者而言，其所購買之軟體，皆有軟體製造商所附上相對應之一軟體序號。該使用者在電腦上安裝該軟體後，即可在該電腦上，使用其所附上之該軟體序號註冊。或是需將該序號告知該軟體製造商並取得一註冊碼，在該軟體將該序號與註冊碼，與出版時儲存有複數個軟體序號及註冊碼之檔案核對無誤後，該使用者才能成為一合法使用者。此註冊方法之缺點是，該軟體可以藉由該序號及該註冊碼，在不同之電腦上安裝使用，因而產生了非法使用之問題。

對上述習知技術產生之問題，有些軟體製造商，會在每一套軟體出版時，附上一硬體之保護鎖(key-pro)。使用者在電腦上安裝該軟體後，還要將保護鎖連結於電腦之介面卡連接埠(connecting port)上，例如印表機埠等，然後在電腦上，使用其所附上之軟體序號與註冊碼註冊，使用者才能成為一合法使用者。此方法之缺點是，保護鎖



五、發明說明 (2)

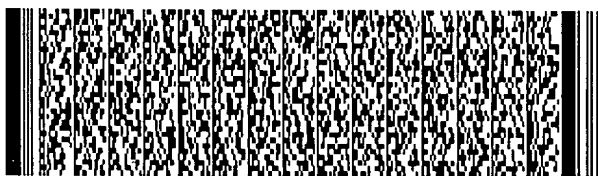
提高了軟體製造廠商的成本，而且對使用者而言，若每一套軟體皆須在電腦上加上一保護鎖，會對電腦硬體空間產生相當大之負擔。更特別的是，有些非法使用者可能破解保護鎖並加以複製，使得軟體可以非法地，在不同之電腦上安裝使用，進而產生了非法使用之問題。

在網際網路發達後，習知的軟體序號註冊之方法，一般是該軟體製造廠商，具有一網址，連接於網際網路上，該網址儲存有複數組序號與註冊碼之對應關係。在使用者購買該軟體並將該軟體安裝於電腦後，需將軟體所附之序號，加上個人身份(user ID)，例如使用者之電子信箱帳號(e-mail address)，藉由網際網路上傳至網址，藉以取得一對應之註冊碼，在網址檢查序號與註冊碼對應相符時，便將序號與使用者身份及註冊碼之對應關係儲存入網址內。使用者才能成為一合法使用者。此註冊方法之缺點是，軟體可以藉由序號、使用者身份及註冊碼，在不同之電腦上安裝使用，而產生了非法使用之問題。

發明內容

因此本發明的目的就是在提供一種應用硬體來偵測非法軟體載入的系統、方法、及其使用之晶片、與具有該晶片之電腦系統及一軟體註冊中心，以避免因非法使用者，利用非法之技術，未經授權非法使用該軟體。

本發明的再一目的是提供一種應用硬體來偵測非法軟體載入的系統、方法、及其使用之晶片、與具有該晶片



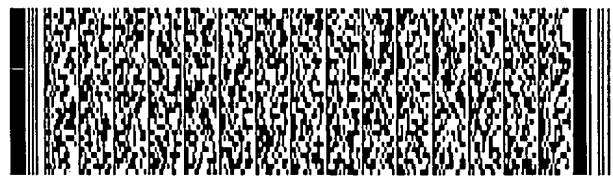
五、發明說明 (3)

之電腦系統及一軟體註冊中心，當使用者非法使用該軟體時，可通知該軟體製造商，以保護其智慧財產權。

為了達成前述之目的，本發明提出一種應用硬體偵測非法軟體載入之系統，適用於一電腦安裝與執行具有一軟體序號之一軟體，該系統至少包括，一身份辨識電路，其用以在該電腦安裝該軟體時，儲存該軟體序號，並對應產生一檢查碼；以及一通訊控制介面，具有一通訊設備序號，用以連接該身份辨識電路至一新產品註冊中心，該新產品註冊中心根據該軟體序號與該通訊設備序號，更新該檢查碼，其中，當該電腦執行該軟體之程式時，該程式會先檢查該檢查碼，若該檢查碼係在一合法使用者狀態時，則該程式會正常執行，若該檢查碼係在一非法使用狀態時，則該程式不會執行而立即關閉。

在上述之實施例中，該身份辨識電路即為一智慧型安全身份(Smart security-ID, "SID")積體電路(IC)，使用者為了取得合法之使用權，需將軟體之序號，註冊至智慧型安全身份積體電路中。此智慧型安全身份積體電路亦可以做為一序號內建模組(Built-in Module)。

更佳的是，上述新產品註冊中心更包括一資料庫，該資料庫包含複數個資料組，其中當接收到該軟體序號與該通訊設備序號時，用以與該些資料組進行比對，若在該資料庫中無法找到與該軟體序號與該通訊設備序號相同之一資料時，則新增對應於該軟體序號與該通訊設備序號之一資料組，並儲存在該資料庫中，更新該檢查碼在該合法使用



五、發明說明 (4)

者狀態。其中該新產品註冊中心連接到一軟體製造商系統，當該新產品註冊中心根據該軟體序號與該通訊設備序號更新該檢查碼為該合法使用者狀態時，亦通知該軟體製造商系統該軟體製造商系統中的另一通訊設備序號不同時，則更新該檢查碼在該非法使用狀態。

在上述之實施例中，其中該通訊控制介面包括一網路介面卡、一無線區域網路、或一全球定位系統。

在上述之實施例中，其中該新產品註冊中心可以連接到一軟體製造商系統，當該新產品註冊中心根據該軟體序號與該通訊設備序號更新該檢查碼為該合法使用者狀態時，亦通知該軟體製造商系統該軟體已經註冊在該新產品註冊中心。

更佳的是，上述之身份辨識電路包括，一微處理器，具有一記憶體，用以在該電腦安裝該軟體時，可產生該檢查碼；一非揮發性記憶體，耦接到該微處理器，用以儲存該檢查碼；以及一媒體存取控制器，耦接到該非揮發性記憶體與該通訊控制介面，用以將該檢查碼傳送到藉由該通訊控制介面傳送到該新產品註冊中心。

如上所述，其中該記憶體為一可抹除可程式唯讀記憶體、一可電性抹除可程式唯讀記憶體、一快閃記憶體、一靜態隨機存取記憶體、與一動態隨機存取記憶體其中之一。



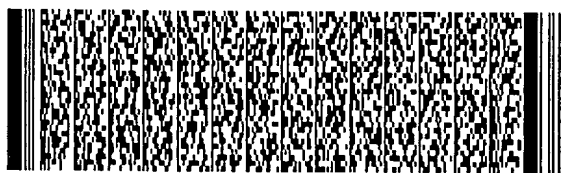
五、發明說明 (5)

如上所述，其中該非揮發性記憶體為一可抹除可程式唯讀記憶體、一可電性抹除可程式唯讀記憶體、與一快閃記憶體其中之一。

在另一實施例中，更佳的是，上述之身份辨識電路包括，一微處理器，用以在該電腦安裝該軟體時，可產生該檢查碼；一非揮發性記憶體，耦接到該微處理器，用以儲存該檢查碼；以及一媒體存取控制器，耦接到該非揮發性記憶體與該通訊控制介面，用以將該檢查碼傳送到藉由該通訊控制介面傳送到該新產品註冊中心。

為了達成本發明之另一目的，提出一種晶片，適用於一偵測非法軟體載入之系統，此系統適用於一電腦安裝與執行具有一軟體序號之一軟體，該晶片包括，一微處理器，用以在該電腦安裝該軟體時，可產生該檢查碼；一非揮發性記憶體，耦接到該微處理器，用以儲存該檢查碼；以及一媒體存取控制器，耦接到該非揮發性記憶體與一通訊控制介面，用以將該檢查碼及其所具有一通訊設備序號傳送到藉由該通訊控制介面傳送到一新產品註冊中心，該新產品註冊中心根據該軟體序號與該通訊設備序號，更該新該檢查碼，其中，當該電腦執行該軟體之程式時，該程式會先檢查該檢查碼，若該檢查碼係在合法使用狀態時，則該程式會正常執行，若該檢查碼係在非法使用狀態時，則該程式不會執行而立即關閉。

如上所述，其中該通訊控制介面包括一網路介面卡、一無線區域網路、與一全球定位系統其中之一。

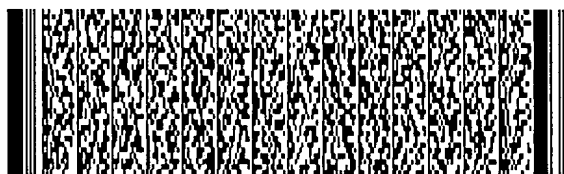


五、發明說明 (6)

如 上 所 述 ， 其 中 該 非 揮 發 性 記 憶 體 為 一 可 抹 除 可 程 式 唯 讀 記 憶 體 、 一 可 電 性 抹 除 可 程 式 唯 讀 記 憶 體 、 與 一 快 閃 記 憶 體 其 中 之 一 。

為達成本發明之另一目的，提出一種應用硬體偵測非法軟體時，該方法適用於以下步驟：當該電腦安裝與執行具有該軟體序號之一儲存該電碼；傳送到該電腦執行該軟體序號中設備程式使用非該序號之儲備式使用者狀態時，該新式會先檢查該程式碼，其中檢查碼，若執行而立即關閉。

如上述，其中該新產品註冊中心更包括一資料庫，該資料庫包含複數個資料組，其當接收該軟體序號與該通訊設備序號時，若該資料庫中無法找到與該軟體序號相同之一使該資料庫時，則新增在該資產產品註冊中心根據該新產品註冊中心軟狀態。其產碼為已該經註冊在該系統，當該新檢查軟體通知該軟體製造商更新該系統。



五、發明說明 (7)

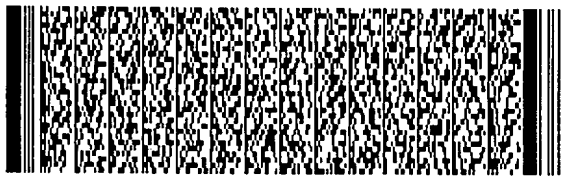
料庫中找到該軟體序號而該通訊設備序號與找到之該資料組中的另一通訊設備序號不同時，則更新該檢查碼在該非法使用狀態。

如上所述，其中將該檢查碼與該電腦所具有之通訊設備序號，傳送到新產品註冊中心之方法係運用有一網路介面、一無線區域網路、與一全球定位系統其中之一。

如上所述，其中該新產品註冊中心連接到一軟體製造商系統，當該新產品註冊中心根據該軟體序號與該通訊設備序號更新該檢查碼為該合法使用者狀態時，亦通知該軟體製造商系統該軟體已註冊在該新產品註冊中心。

為了達成本發明之另一目的，提出一種電腦系統，適用於偵測非法軟體載入之一系統，此系統適用於一電腦安插與執行具有一軟體序號之一軟體，該電腦包括一微處理器，用以在該電腦安裝該軟體時，可產生該檢查碼；以及一記憶體，耦接到該微處理器，用以儲存該檢查碼；以及一媒體存取控制裝置，耦接到該非揮發性記憶體與一通訊控制介面，用以將該檢查碼及其所具有一通訊設備序號傳送到藉由該通訊控制介面傳送該軟體序號與該通訊設備序號，該新產品註冊中心根據該軟體序號與該檢查碼，更新該檢查碼，其中，當該電腦執行該檢查碼時，該程式會先檢查該檢查碼，若該檢查碼係在合法使用狀態時，則該程式會正常執行，若該檢查碼係在非法使用狀態時，則該程式不會執行而立即關閉。

如上所述，其中該通訊控制介面包括一網路介面卡、



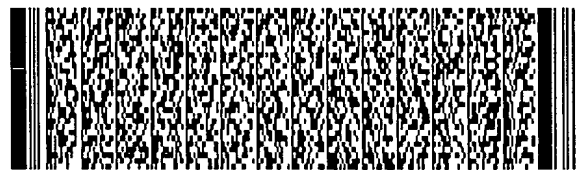
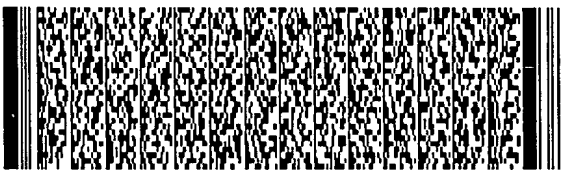
五、發明說明 (8)

一無線區域網路、與一全球定位系統其中之一。

如上述，其中該非揮發性記憶體為一可抹除可程式唯讀記憶體、一可電性抹除可程式唯讀記憶體、與一快閃記憶體其中之一。

為了達成本發明之另一目的，提出一種軟體註冊中心，其適用於具有軟體序號之一硬體偵測，非法軟體載入之電腦安裝一與執行具有一軟體序號之軟體，該軟體註冊中心包括由該資料庫，該資料庫包含複數個資料組，其中當接收到由該電腦在所傳送之該軟體序號與該通訊設備序號時，用以與該些資料組進行比對，該電腦根據該軟體序號與該通訊設備序號，更新儲存於該電腦之檢查碼，其檢查碼，當該電腦執行該軟體時，該軟體之程式會先檢查該檢查碼，若該檢查碼係在該軟體之合法使用狀態時，則該程式正常執行，若該檢查碼係在該軟體之非法使用狀態時，則該程式不會執行而立即關閉。

如上述，其中當接收到該軟體序號與該通訊設備序號時，用以與該些資料組進行比對，若該資料組中無法找到與該軟體序號與該通訊設備序號相同之一資料時，則新儲增對應該軟體序號與該通訊設備序號之一資料組，並其產存中該新產品註冊中心新連接到一軟體製造商系統，當該新檢查碼為該合法使用者狀態時，亦通知該軟體製造商系統該軟體已經註冊在該新產品註冊中心。若該資料組中找到該



五、發明說明 (9)

軟體序號而該通訊設備序號與找到之該資料組中的另一通訊設備序號不同時，則更新該檢查碼與該電腦所具有之通訊設備序號，傳送到該新產品註冊中心之方法係運用之一網路介面、一無線區域網路、與一全球定位系統其中之一。

如上所述，其中該新產品註冊中心連接到一軟體製造商系統，當該新產品註冊中心根據該軟體序號與該通訊設備序號更新該檢查碼為該合法使用者狀態時，亦通知該軟體製造商系統該軟體已經註冊在該新產品註冊中心。

如上所述，其中該新產品註冊中心連接到一軟體製造商系統，當該新產品註冊中心根據該軟體序號與該通訊設備序號更新該檢查碼為該合法使用者狀態時，亦通知該軟體製造商系統該軟體已經註冊在該新產品註冊中心。

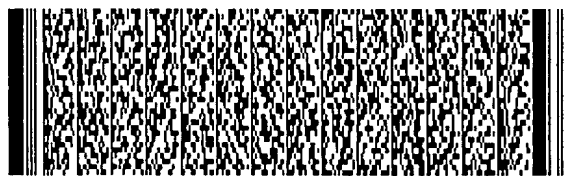
本發明因採用上述發明之一種應用硬體來偵測非法軟體載入的系統與方法，因此可以避免因非法使用非法軟體之技術，未經授權非法使用軟體。更可保護軟體製造商之智慧財產權。

本發明因採用上述發明之一種應用硬體來偵測非法軟體載入的系統與方法，因此當有非法使用者，非法使用軟體時，該應用硬體可以偵測到並通知該軟體製造廠商。更可保護軟體製造商之權益。

為讓本發明之上述和其他目的、特徵、和優點能更明顯易懂，下文特舉一較佳實施例，並配合所附圖式，作詳細說明如下：

實施方式：

首先，請參照第1圖，係本實施例中在一電腦10中具有應用硬體來偵測非法軟體載入功能之裝置100之方塊示

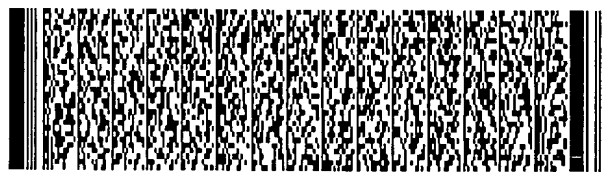
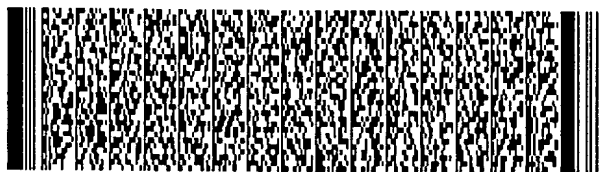


五、發明說明 (10)

意圖。此裝置100包括一身份辨識電路102與一通訊控制介面104。此通訊控制介面104係讓此身份辨識電路102與外界溝通之媒介，而其通連之方式可為無線通信、有線通信以及其他任何可傳送資料之方式。

上述之身份辨識電路102至少包括了一微處理器106、一記憶體108、一媒體存取控制器110以及一非揮發性記憶體112。圖示中記憶體108係耦接到微處理器106，然而，在另一實施例中，此記憶體108可為微處理器106內部所內建之記憶體。微處理器106在電腦安裝一軟體時，可產生一檢查碼。而非揮發性記憶體112可以在電腦安裝軟體時，將其軟體序號(Serial Number，底下簡稱"S/N")以及微處理器106產生之檢查碼儲存於其中。

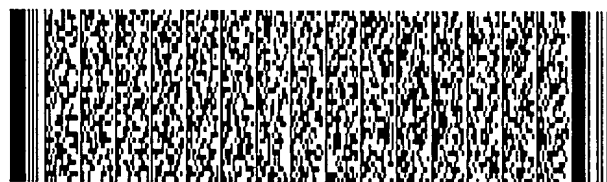
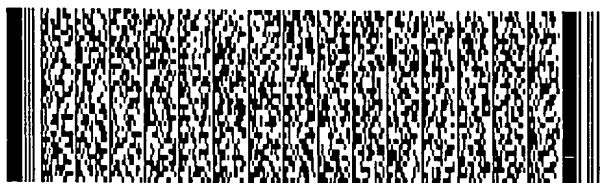
請參照第1圖，其中上述的記憶體108可以為一可抹除可程式唯讀記憶體(Erasable PROM, "EPROM")、一可電性抹除可程式唯讀記憶體(Electrically Erasable PROM, "EEPROM")、一快閃記憶體(Flash memory)、一靜態隨機存取記憶體(Static Random Access Memory, "SRAM")，以及一動態隨機存取記憶體(Dynamic Random Access Memory, "DRAM")。其中非揮發性記憶體112可為一快閃記憶體(Flash memory)、一可抹除可程式唯讀記憶體、或是一可電性抹除可程式唯讀記憶體。而通訊控制介面104在一較佳實施例中可為一網路介面設備。而在其他選擇之實施例中，可為一無線區域網路或一全球定位系統等等通信設備。



五、發明說明 (11)

請參照第1圖，其中身份辨識電路102係一種用來偵測非法軟體載入的硬體裝置。當電腦安裝與執行具有軟體序號S/N之軟體時，若是偵測到沒有身份辨識電路102，則停止安裝。若是偵測到存在身份辨識電路102，則可開始在此電腦上安裝軟體，並將軟體序號S/N儲存於身份辨識電路102中，接著產生一檢查碼（在一實施例中，此檢查碼之初始值設為1）。請配合第4圖說明，此第4圖係繪示使用者執行軟體SW之程式時，此程式會先連結至身份辨識電路102，檢查所儲存之檢查碼cd之值。若檢查碼cd之值為1，則程式會正常執行，反之，若檢查碼cd之值為0，則程式不會執行，會立即關閉。而此檢查碼cd之設定，詳細說明如下。

在本實施例之偵測非法軟體載入的系統中，除了上述之裝置100外，更包括一新產品註冊中心114，其具有一資料庫116。此新產品註冊中心114係藉由通訊控制介面104與具有應用硬體來偵測非法軟體載入功能之裝置100作通聯，而此通聯之方式可以是經由一網路介面卡設備。而在其他選擇之實施例中，亦可為一無線區域網路介面卡或一全球定位系統等等任何具有可將通訊控制介面104與新產品註冊中心114相連接傳送資料之方法。在本發明一選擇實施例中，此新產品註冊中心114更可與軟體製造商系統118相通連，可互相傳送資料，例如傳送目前登錄之軟體使用者資料，或是在有異常之情形，也就是有任何盜用之情形下，可進行資料之傳送。



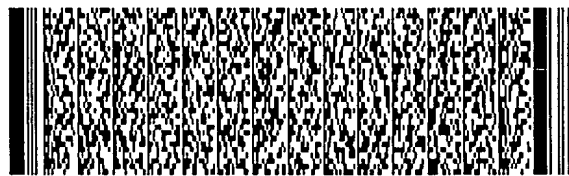
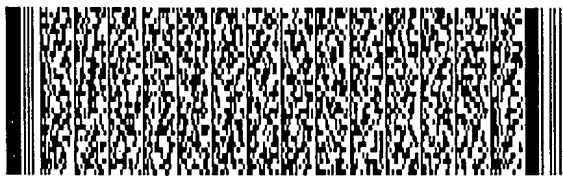
五、發明說明 (12)

請參照第2圖，係顯示新產品註冊中心114之資料庫116中所儲存之資料組之一例，其中資料庫116具有複數個資料組。每一資料組包括軟體製造商代碼、軟體序號、通訊設備序號以及檢查碼。新產品註冊中心114係透過通訊控制介面104與電腦連結，新產品註冊中心114亦與軟體製造商系統118連結。

當軟體SW在電腦上完成其安裝程序後，透過通訊控制介面104，傳輸軟體序號S/N、電腦之一通訊設備序號S1以及檢查碼cd至新產品註冊中心114。此通訊設備序號S1係可用以辨識此電腦之序號，一般而言，若通訊控制介面104為一網路卡介面設備，則此通訊設備序號S1在一較佳實施例中為網路卡之序號。而在其他選擇之實施例中，若通訊控制介面104為一無線區域網路介面，則為無線網路卡之序號。而若是通訊控制介面104為一全球定位系統，則可為此全球定位系統中辨識此通訊控制介面104之序號等等。當然，此通訊設備序號S1亦可定義為電腦獨特之序號。

若軟體序號S/N不包括於資料庫116之任一組資料組中，則開始進行新使用軟體之註冊流程。此註冊流程包括由新產品註冊中心114依據軟體SW選取一軟體製造商代碼，將軟體製造商代碼，連同傳輸來之軟體序號S/N、通訊設備序號S1以及檢查碼cd，儲存在一新的資料組中。並定義此檢查碼為1，也就是在一合法使用者之狀態。

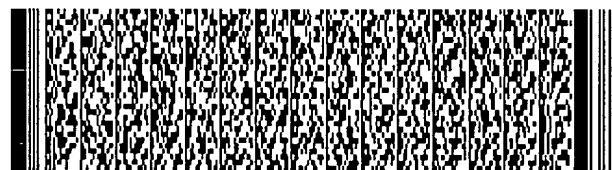
若軟體序號S/N已包括於資料庫116之某一組資料組



五、發明說明 (13)

中，但通訊設備序號S1不同於此資料組中之通訊設備序號，則新產品註冊中心114將傳輸來之檢查碼cd之值設為0，並將此值回傳至偵測非法軟體載入功能之裝置100，並將裝置100中之檢查碼cd之值設定為0。如前所述，當使用者執行已安裝之軟體之程式時，程式會先連結至身份辨識電路102，檢查檢查碼cd之值。若檢查碼cd之值為1，則此程式會正常執行；若檢查碼cd之值為0，則此程式不會執行，會立即關閉。

第3圖繪示本發明一較佳實施例中之一種應用身份辨識電路來偵測非法軟體載入之方法之流程圖。首先，請參照第3圖，係本發明提出之一種應用身份辨識電路來偵測非法軟體載入的方法，適用於第1圖所繪示之系統。此系統具有當將具有一軟體序號S/N之軟體SW安裝於一電腦時，偵測是否為非法使用之功能。而此具有偵測非法軟體載入功能之裝置100包括一身份辨識電路102與一具有通訊設備序號S1之通訊控制介面104。而此系統中更包括具有資料庫116之新產品註冊中心114。除此之外，在一選擇實施例中，更可包括一軟體製造商系統118。其中此電腦係透過裝置100，與新產品註冊中心114連結，新產品註冊中心114亦與軟體製造商系統118連結。資料庫116具有複數個資料組，如第2圖所示，每一資料組為一組資料包括一軟體製造商代碼、一軟體序號、一通訊設備序號以及一檢查碼。應用身份辨識電路102來偵測非法軟體載入的方法如下所述：



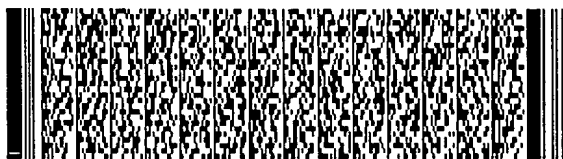
五、發明說明 (14)

當電腦安裝軟體SW時，需輸入其軟體序號S/N。軟體SW會傳輸軟體序號S/N至通訊設備100。此時若軟體SW與通訊設備100之身份辨識電路102無法連結或通訊設備100不具有身份辨識電路102，則軟體SW停止其安裝程序。若軟體SW連結上通訊設備100之身份辨識電路102，則繼續進行以下步驟。

軟體SW將軟體序號S/N儲存於身份辨識電路102中、完成其安裝程序、產生一檢查碼cd（起始值設為1）並啟動通訊設備100，傳輸軟體序號S/N、通訊設備100之一通訊設備序號S1以及檢查碼cd至新產品註冊中心114。

新產品註冊中心114將軟體序號S/N及通訊設備序號S1，與新產品註冊中心114內之資料庫116之每一資料組之軟體序號及通訊設備序號比對。若軟體序號S/N不包括於資料庫116之任一組資料組中，則新產品註冊中心114將依據軟體SW選取一軟體製造商代碼，將軟體製造商代碼，連同傳輸來之軟體序號S/N、通訊設備序號S1以及檢查碼cd，儲存在一新的資料組中。此時更包括連結至軟體製造商系統118，並對其告知該電腦為一非法使用者。

若軟體序號S/N已包括於資料庫116之某一組資料組中，但通訊設備序號S1不同於該某一組資料組中之該通訊設備序號，則新產品註冊中心114將傳輸來之檢查碼cd之值設為0並將此值回傳至通訊設備100，並將通訊設備100中之檢查碼cd之值設為0。此時更包括連結至軟體製造商系統118，並對其告知該電腦為一合法使用者。



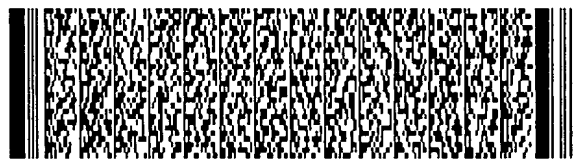
五、發明說明 (15)

同樣地，請參照第4圖，第4圖繪示使用者執行該軟體SW之程式PR之方法。當該電腦執行程式PR時，該程式PR會先連結至該身份辨識電路102，檢查檢查碼cd之值；若檢查碼cd之值為1，則程式PR會正常執行；若檢查碼cd之值為0，則程式PR不會執行，會立即關閉。

如上所述，其中將該檢查碼與該電腦所具有之通訊設備序號，傳送到該新產品註冊中心之方法係運用一網路介面、一無線區域網路、與一全球定位系統其中之一。

如上所述，其中該新產品註冊中心連接到一軟體製造商系統，當該新產品註冊中心根據該軟體序號與該通訊設備序號更新該檢查碼為該合法使用者狀態時，亦通知該軟體製造商系統該軟體已經註冊在該新產品註冊中心。

雖然本發明已以一較佳實施例揭露如上，然其並非用以限定本發明，任何熟習此技藝者，在不脫離本發明之精神和範圍內，當可作些許之更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。



圖式簡單說明

第1圖係繪示依照本發明一較佳實施例之一種具有身份辨識電路之裝置示意圖；

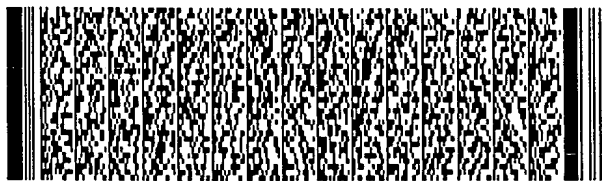
第2圖係繪示運用於第1圖中之具有身份辨識電路之系統中之新產品註冊中心之資料庫中所儲存之資料組；

第3圖係繪示依照本發明一較佳實施例之一種應用身份辨識電路來偵測非法軟體載入的方法之示意圖；以及

第4圖係繪示依照本發明一較佳實施例之使用者執行軟體之程式之步驟。

圖式標記說明：

- 10：電腦
- 100：通訊設備
- 102：身份辨識電路
- 104：通訊控制介面
- 106：微處理器
- 108：記憶體
- 110：媒體存取控制器
- 112：非揮發性記憶體
- 114：新產品註冊中心
- 116：資料庫
- 118：軟體製造商



六、申請專利範圍

1. 一種應用硬體偵測非法軟體載入之系統，適用於一電腦安裝與執行具有一軟體序號之一軟體，該系統包括：

一身份辨識電路，其用以在該電腦安裝該軟體時，儲存該軟體序號，並對應產生一檢查碼；以及

一通訊控制介面，具有一通訊設備序號，用以連接該身份辨識電路至一新產品註冊中心，該新產品註冊中心根據該軟體序號與該通訊設備序號，更新該檢查碼，其中，當該電腦執行該軟體之程式時，該程式會先檢查該檢查碼，若該檢查碼係在一合法使用者狀態時，則該程式會正常執行，若該檢查碼係在一非法使用狀態時，則該程式不會執行而立即關閉。

2. 如申請專利範圍第1項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該新產品註冊中心更包括一資料庫，該資料庫包含複數個資料組，其中當接收到該軟體序號與該通訊設備序號時，用以與該些資料組進行比對，若在該資料庫中無法找到與該軟體序號與該通訊設備序號相同之資料時，則新增對應於該軟體序號與該通訊設備序號之一資料組，並儲存在該資料庫中，更新該檢查碼在該合法使用者狀態。

3. 如申請專利範圍第2項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該新產品註冊中心連接到一軟體製造商系統，當該新產品註冊中心根據該軟體序號與該通訊設備序號更新該檢查碼為該合法使用者狀態時，



六、申請專利範圍

亦通知該軟體製造商系統該軟體已經註冊在該新產品註冊中心。

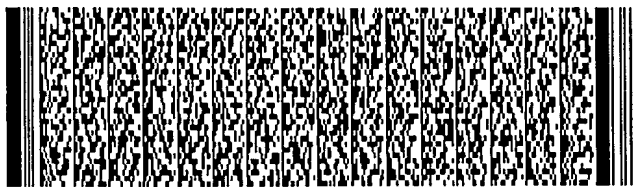
4. 如申請專利範圍第1項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該新產品註冊中心更包括一資料庫，該資料庫包含複數個資料組，其中當接收到該軟體序號與該通訊設備序號時，用以與該些資料組進行比對，若在該資料庫中找到該軟體序號而該通訊設備序號與找到之該資料組中的另一通訊設備序號不同時，則更新該檢查碼在該非法使用狀態。

5. 如申請專利範圍第1項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該通訊控制介面包括一網路介面卡。

6. 如申請專利範圍第1項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該通訊控制介面包括一無線區域網路。

7. 如申請專利範圍第1項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該通訊控制介面包括一全球定位系統。

8. 如申請專利範圍第1項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該新產品註冊中心連接到一軟體製造商系統，當該新產品註冊中心根據該軟體序號與該通訊設備序號更新該檢查碼為該合法使用者狀態時，亦通知該軟體製造商系統該軟體已經註冊在該新產品註冊中心。



六、申請專利範圍

9. 如申請專利範圍第1項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該身份辨識電路包括：

一微處理器，具有一記憶體，用以在該電腦安裝該軟體時，可產生該檢查碼；

一非揮發性記憶體，耦接到該微處理器，用以儲存該檢查碼；以及

一媒體存取控制器，耦接到該非揮發性記憶體與該通訊控制介面，用以將該檢查碼傳送到藉由該通訊控制介面傳送到該新產品註冊中心。

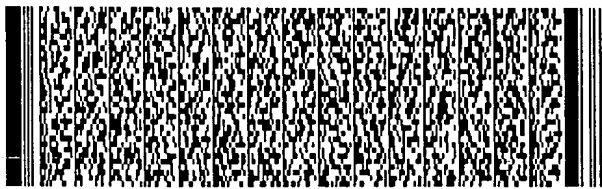
10. 如申請專利範圍第9項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該記憶體為一可抹除可程式唯讀記憶體。

11. 如申請專利範圍第9項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該記憶體為一可電性抹除可程式唯讀記憶體。

12. 如申請專利範圍第9項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該記憶體為一快閃記憶體。

13. 如申請專利範圍第9項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該記憶體為一靜態隨機存取記憶體。

14. 如申請專利範圍第9項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該記憶體為一動態隨機存取記憶體。



六、申請專利範圍

15. 如申請專利範圍第9項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該非揮發性記憶體為一可抹除可程式唯讀記憶體。

16. 如申請專利範圍第9項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該非揮發性記憶體為一可電性抹除可程式唯讀記憶體。

17. 如申請專利範圍第9項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該非揮發性記憶體為一快閃記憶體。

18. 如申請專利範圍第1項所述之應用身份辨識電路來偵測非法軟體載入的系統，其中該身份辨識電路包括：

- 一微處理器，用以在該電腦安裝該軟體時，可產生該檢查碼；

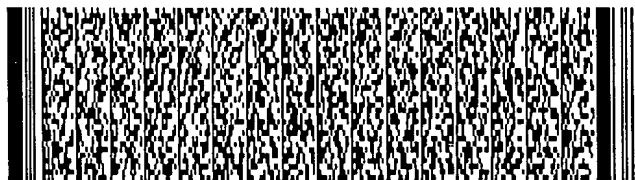
- 一非揮發性記憶體，耦接到該微處理器，用以儲存該檢查碼；以及

- 一媒體存取控制器，耦接到該非揮發性記憶體與該通訊控制介面，用以將該檢查碼傳送到藉由該通訊控制介面傳送到該新產品註冊中心。

19. 一種晶片，適用於一偵測非法軟體載入之系統，此系統適用於一電腦安裝與執行具有一軟體序號之一軟體，該晶片包括：

- 一微處理器，用以在該電腦安裝該軟體時，可產生該檢查碼；

- 一非揮發性記憶體，耦接到該微處理器，用以儲存



六、申請專利範圍

該檢查碼；以及

一媒體存取控制器，耦接到該非揮發性記憶體與一通訊控制介面，用以將該檢查碼及其所具有之一通訊設備序號傳送到藉由該通訊控制介面傳送到一新產品註冊中心，該新產品註冊中心根據該軟體序號與該通訊設備序號，更新該檢查碼，其中，當該電腦執行該軟體之程式時，該程式會先檢查該檢查碼，若該檢查碼係在一合法使用者狀態時，則該程式會正常執行，若該檢查碼係在一非法使用狀態時，則該程式不會執行而立即關閉。

20. 如申請專利範圍第19項所述之晶片，其中該通訊控制介面包括一網路介面卡。

21. 如申請專利範圍第19項所述之晶片，其中該通訊控制介面包括一無線區域網路。

22. 如申請專利範圍第19項所述之晶片，其中該通訊控制介面包括一全球定位系統。

23. 如申請專利範圍第19項所述之晶片，其中該非揮發性記憶體為一可抹除可程式唯讀記憶體。

24. 如申請專利範圍第19項所述之晶片，其中該非揮發性記憶體為一可電性抹除可程式唯讀記憶體。

25. 如申請專利範圍第19項所述之晶片，其中該非揮發性記憶體為一快閃記憶體。

26. 一種應用硬體偵測非法軟體載入之方法，適用於一電腦安裝與執行具有一軟體序號之一軟體，該方法包括：



六、申請專利範圍

當該電腦安裝該軟體時，儲存該軟體序號，並對應產生一檢查碼；以及

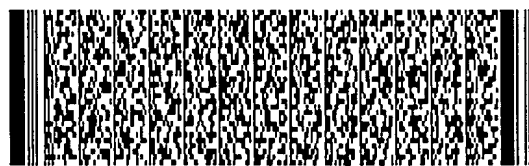
將該檢查碼與該電腦所具有之一通訊設備序號，傳送到一新產品註冊中心；

該新產品註冊中心根據該軟體序號與該通訊設備序號，更新該檢查碼，其中，當該電腦執行該軟體之程式時，該程式會先檢查該檢查碼，若該檢查碼係在一合法使用者狀態時，則該程式會正常執行，若該檢查碼係在一非法使用狀態時，則該程式不會執行而立即關閉。

27. 如申請專利範圍第26項所述之應用硬體偵測非法軟體載入之方法，其中該新產品註冊中心更包括一資料庫，該資料庫包含複數個資料組，其中當接收到該軟體序號與該通訊設備序號時，用以與該些資料組進行比對，若該資料庫中無法找到與該軟體序號與該通訊設備序號相同之資料時，則新增對應於該軟體序號與該通訊設備序號之一資料組，並儲存在該資料庫中，更新該檢查碼在該合法使用者狀態。

28 如申請專利範圍第27項所述之應用硬體偵測非法軟體載入之方法，其中該新產品註冊中心連接到一軟體製造商系統，當該新產品註冊中心根據該軟體序號與該通訊設備序號更新該檢查碼為該合法使用者狀態時，亦通知該軟體製造商系統該軟體已經註冊在該新產品註冊中心。

29. 如申請專利範圍第26項所述之應用硬體偵測非法軟體載入之方法，其中該新產品註冊中心更包括一資料



六、申請專利範圍

庫，該資料庫包含複數個資料組，其中當接收到該軟體序號與該通訊設備序號時，用以與該些資料組進行比對，若在該資料庫中找到該軟體序號而該通訊設備序號與找到之該資料組中的另一通訊設備序號不同時，則更新該檢查碼在該非法使用狀態。

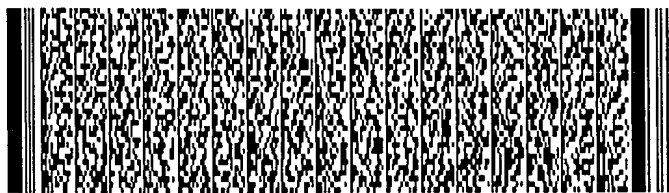
30. 如申請專利範圍第26項所述之應用硬體偵測非法軟體載入之方法，其中將該檢查碼與該電腦所具有之通訊設備序號，傳送到新產品註冊中心之方法係運用一網路介面。

31. 如申請專利範圍第26項所述之應用硬體偵測非法軟體載入之方法，其中將該檢查碼與該電腦所具有之通訊設備序號，傳送到該新產品註冊中心之方法係運用一無線區域網路。

32. 如申請專利範圍第26項所述之應用硬體偵測非法軟體載入之方法，其中將該檢查碼與該電腦所具有之通訊設備序號，傳送到新產品註冊中心之方法係運用一全球定位系統。

33. 如申請專利範圍第26項所述之應用硬體偵測非法軟體載入之方法，其中該新產品註冊中心連接到一軟體製造商系統，當該新產品註冊中心根據該軟體序號與該通訊設備序號更新該檢查碼為該合法使用者狀態時，亦通知該軟體製造商系統該軟體已經註冊在該新產品註冊中心。

34. 一種電腦系統，適用於一偵測非法軟體載入之系統，此系統適用於一電腦安裝與執行具有一軟體序號之一



六、申請專利範圍

軟體，該電腦包括：

一微處理器，用以在該電腦安裝該軟體時，可產生該檢查碼；

一非揮發性記憶體，耦接到該微處理器，用以儲存該檢查碼；以及

一媒體存取控制器，耦接到該非揮發性記憶體與一通訊控制介面，用以將該檢查碼及其所具有之一通訊設備序號傳送到藉由該通訊控制介面傳送到一新產品註冊中心，該新產品註冊中心根據該軟體序號與該通訊設備序號，更新該檢查碼，其中，當該電腦執行該軟體之程式時，該程式會先檢查該檢查碼，若該檢查碼係在一合法使用者狀態時，則該程式會正常執行，若該檢查碼係在一非法使用狀態時，則該程式不會執行而立即關閉。

35. 如申請專利範圍第34項所述之電腦系統，其中該通訊控制介面包括一網路介面卡。

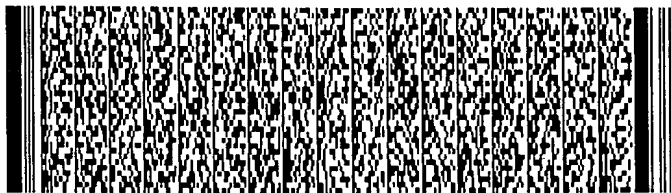
36. 如申請專利範圍第34項所述之電腦系統，其中該通訊控制介面包括一無線區域網路。

37. 如申請專利範圍第34項所述之電腦系統，其中該通訊控制介面包括一全球定位系統。

38. 如申請專利範圍第34項所述之電腦系統，其中該非揮發性記憶體為一可抹除可程式唯讀記憶體。

39. 如申請專利範圍第34項所述之電腦系統，其中該非揮發性記憶體為一可電性抹除可程式唯讀記憶體。

40. 如申請專利範圍第34項所述之電腦系統，其中該



六、申請專利範圍

非揮發性記憶體為一快閃記憶體。

41. 一種軟體註冊中心，其適用於具有應用硬體偵測非法軟體載入之電腦安裝與執行具有一軟體序號之一軟體，該軟體註冊中心包括一資料庫，該資料庫包含複數個資料組，其中當接收到由該電腦在所傳送之該軟體序號與對應於該電腦之一通訊設備序號時，用以與該些資料組進行比對，並根據該軟體序號與該通訊設備序號，更新儲存於該電腦之一檢查碼，其中，當該電腦執行該軟體之程式時，該程式會先檢查該檢查碼，若該檢查碼係在一合法使用者狀態時，則該程式會正常執行，若該檢查碼係在一非法使用狀態時，則該程式不會執行而立即關閉。

42. 如申請專利範圍第41項所述之軟體註冊中心，其中當接收到該軟體序號與該通訊設備序號時，用以與該些資料組進行比對，若該資料庫中無法找到與該軟體序號與該通訊設備序號相同之資料時，則新增對應於該軟體序號與該通訊設備序號之一資料組，並儲存在該資料庫中，更新該檢查碼在該合法使用者狀態。

43. 如申請專利範圍第42項所述之軟體註冊中心，其中該新產品註冊中心連接到一軟體製造商系統，當該新產品註冊中心根據該軟體序號與該通訊設備序號更新該檢查碼為該合法使用者狀態時，亦通知該軟體製造商系統該軟體已經註冊在該新產品註冊中心。

44. 如申請專利範圍第41項所述之軟體註冊中心，其中當接收到該軟體序號與該通訊設備序號時，用以與該些



六、申請專利範圍

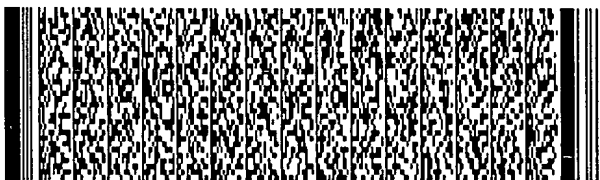
資料組進行比對，若在該資料庫中找到該軟體序號而該通訊設備序號與找到之該資料組中的另一通訊設備序號不同時，則更新該檢查碼在該非法使用狀態。

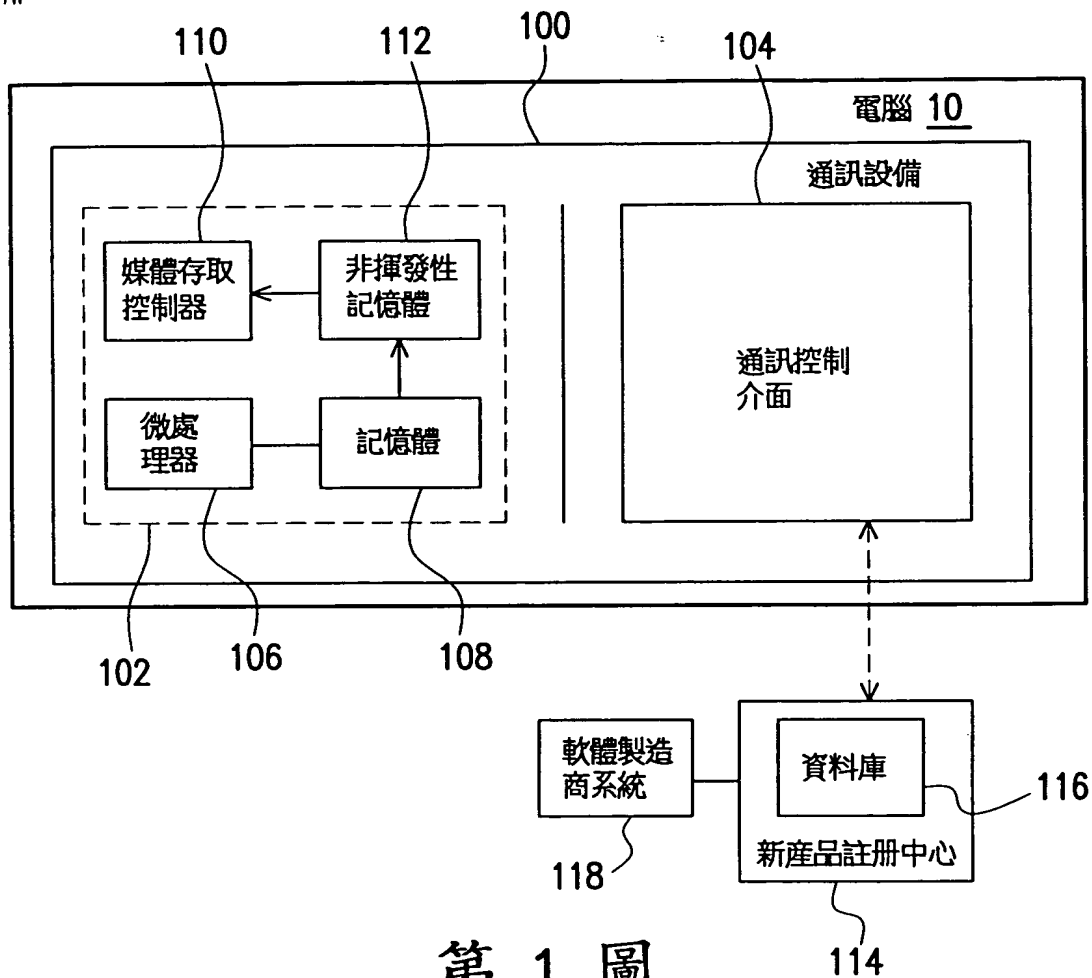
45. 如申請專利範圍第41項所述之軟體註冊中心，其中將該檢查碼與該電腦所具有之通訊設備序號，傳送到該新產品註冊中心之方法係運用一網路介面。

46. 如申請專利範圍第41項所述之軟體註冊中心，其中將該檢查碼與該電腦所具有之通訊設備序號，傳送到該新產品註冊中心之方法係運用一無線區域網路。

47. 如申請專利範圍第41項所述之軟體註冊中心，其中將該檢查碼與該電腦所具有之通訊設備序號，傳送到該新產品註冊中心之方法係運用一全球定位系統。

48. 如申請專利範圍第41項所述之軟體註冊中心，其中該新產品註冊中心連接到一軟體製造商系統，當該新產品註冊中心根據該軟體序號與該通訊設備序號更新該檢查碼為該合法使用者狀態時，亦通知該軟體製造商系統該軟體已經註冊在該新產品註冊中心。

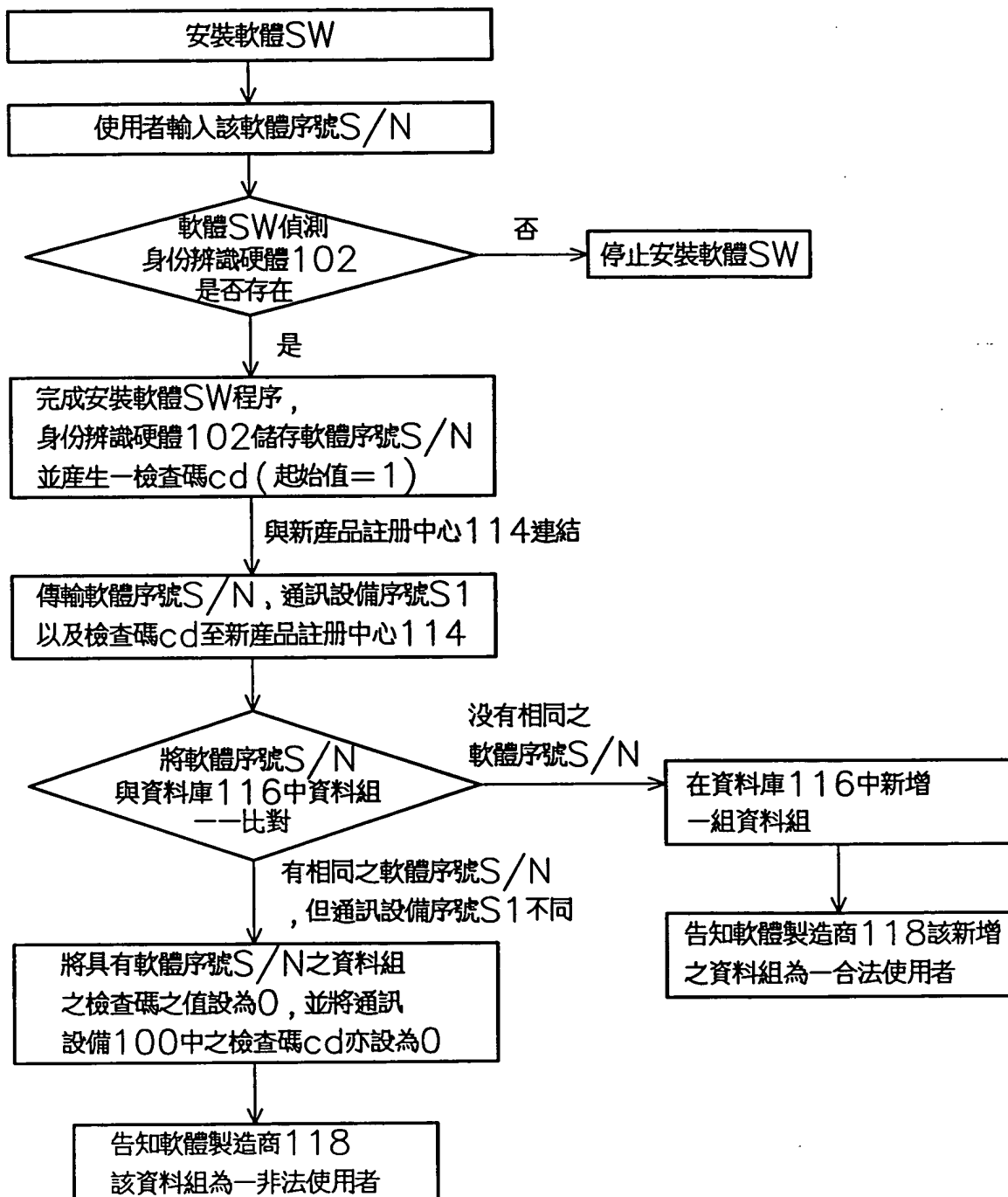




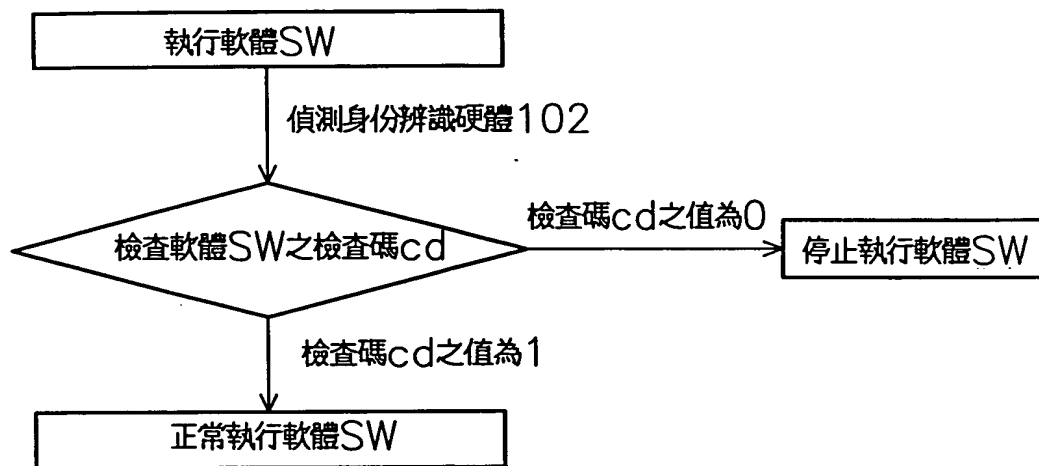
第 1 圖

軟體製造商	軟體製造商代碼	軟體序號	通訊設備序號	檢查碼
Microsoft	00001	AAAAAA	BBBBBB	1
Adobe	00002	CCCCC	DDDDDD	1
Micromedia	00003	EEEEEE	FFFFFF	1
...
...

第 2 圖

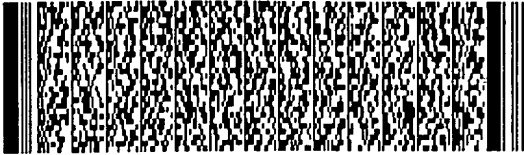


第 3 圖

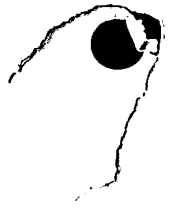
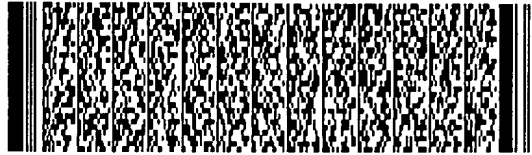


第 4 圖

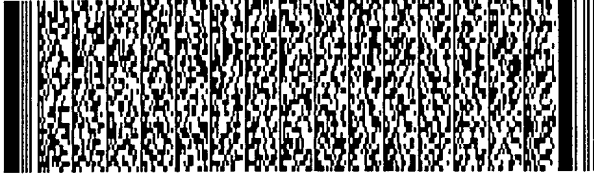
第 1/30 頁



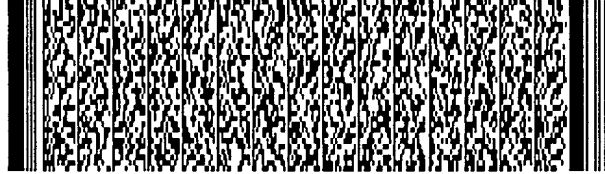
第 1/30 頁



第 2/30 頁



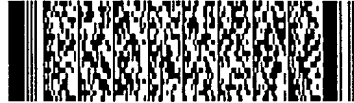
第 2/30 頁



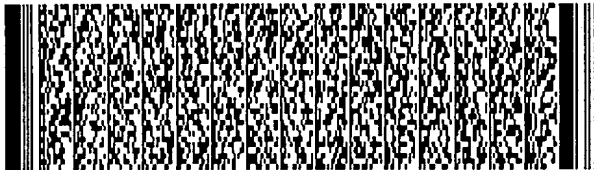
第 3/30 頁



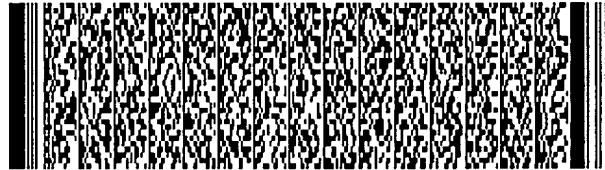
第 4/30 頁



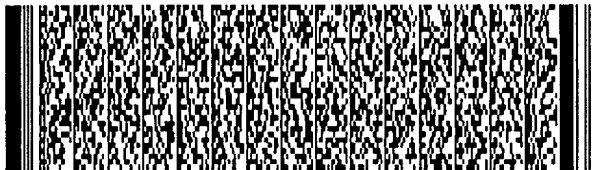
第 5/30 頁



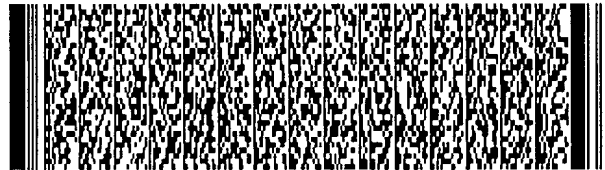
第 5/30 頁



第 6/30 頁



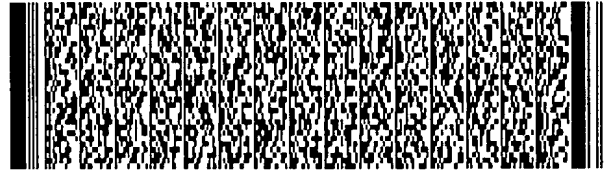
第 6/30 頁



第 7/30 頁



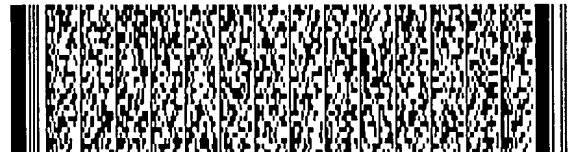
第 7/30 頁



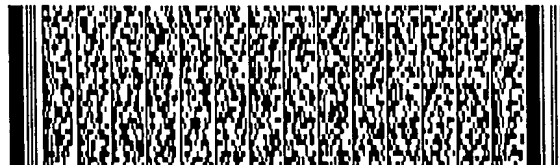
第 8/30 頁



第 8/30 頁



第 9/30 頁



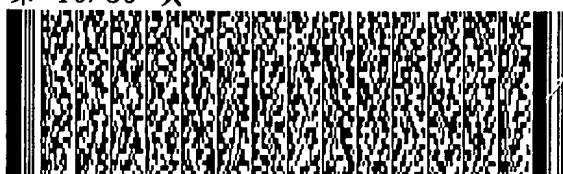
第 9/30 頁



第 10/30 頁



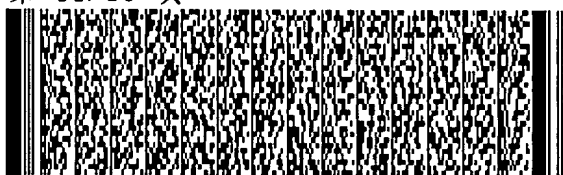
第 10/30 頁



第 11/30 頁



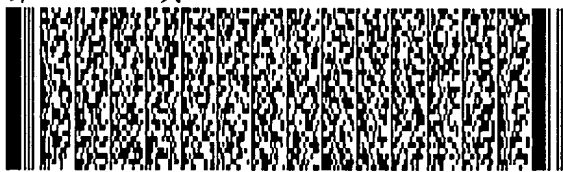
第 11/30 頁



第 12/30 頁



第 12/30 頁



第 13/30 頁



第 13/30 頁



第 14/30 頁



第 14/30 頁



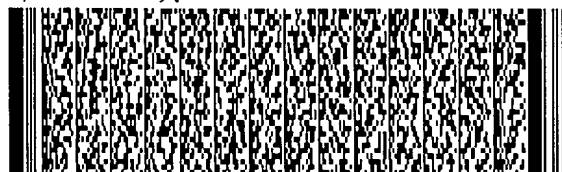
第 15/30 頁



第 15/30 頁



第 16/30 頁



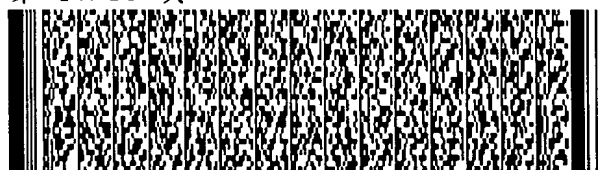
第 16/30 頁



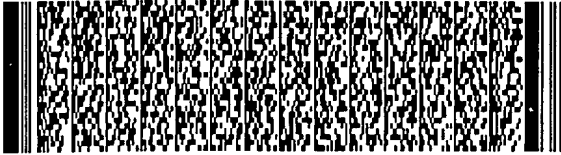
第 17/30 頁



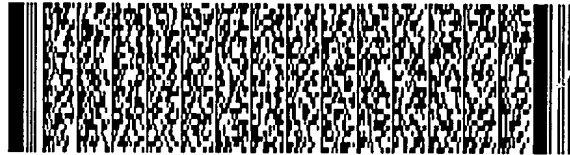
第 17/30 頁



第 18/30 頁



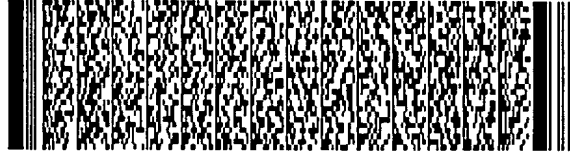
第 18/30 頁



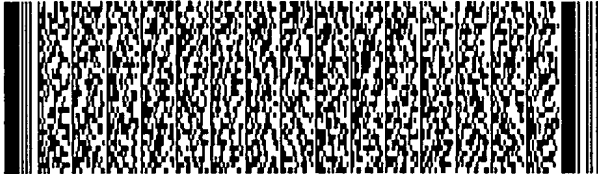
第 19/30 頁



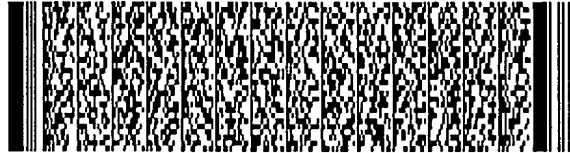
第 19/30 頁



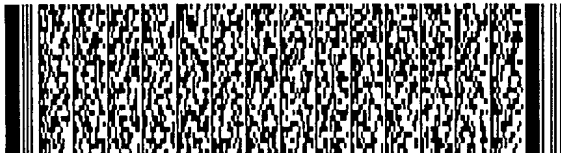
第 20/30 頁



第 21/30 頁



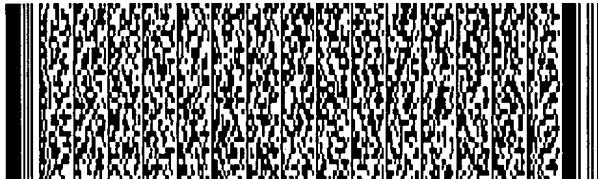
第 21/30 頁



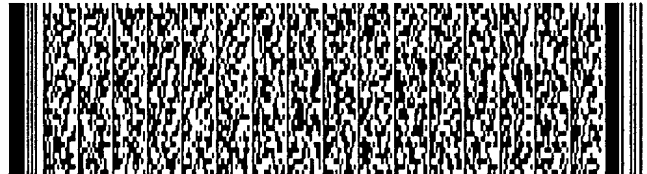
第 22/30 頁



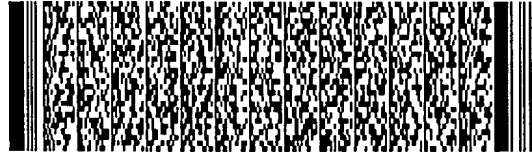
第 23/30 頁



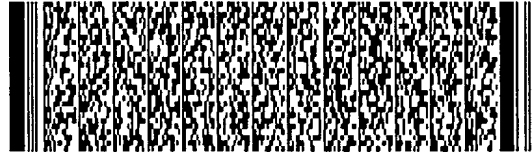
第 24/30 頁



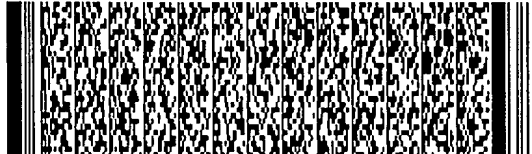
第 25/30 頁



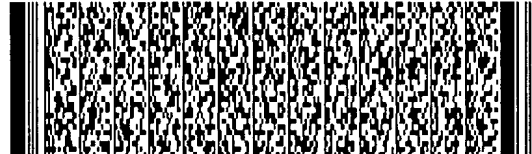
第 25/30 頁



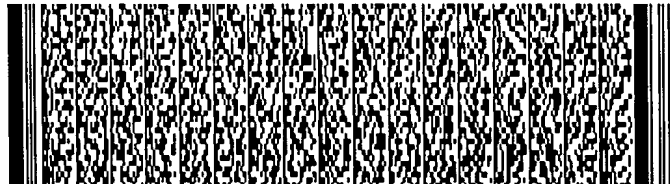
第 26/30 頁



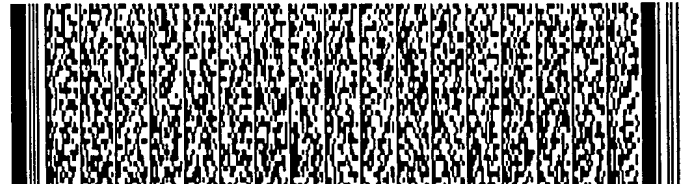
第 26/30 頁



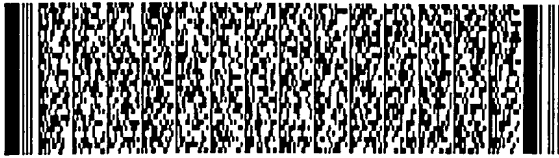
第 27/30 頁



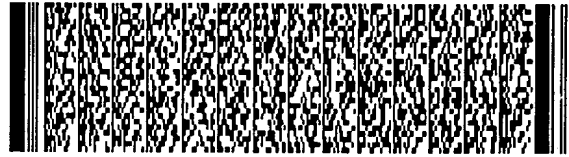
第 28/30 頁



第 29/30 頁



第 29/30 頁



第 30/30 頁

